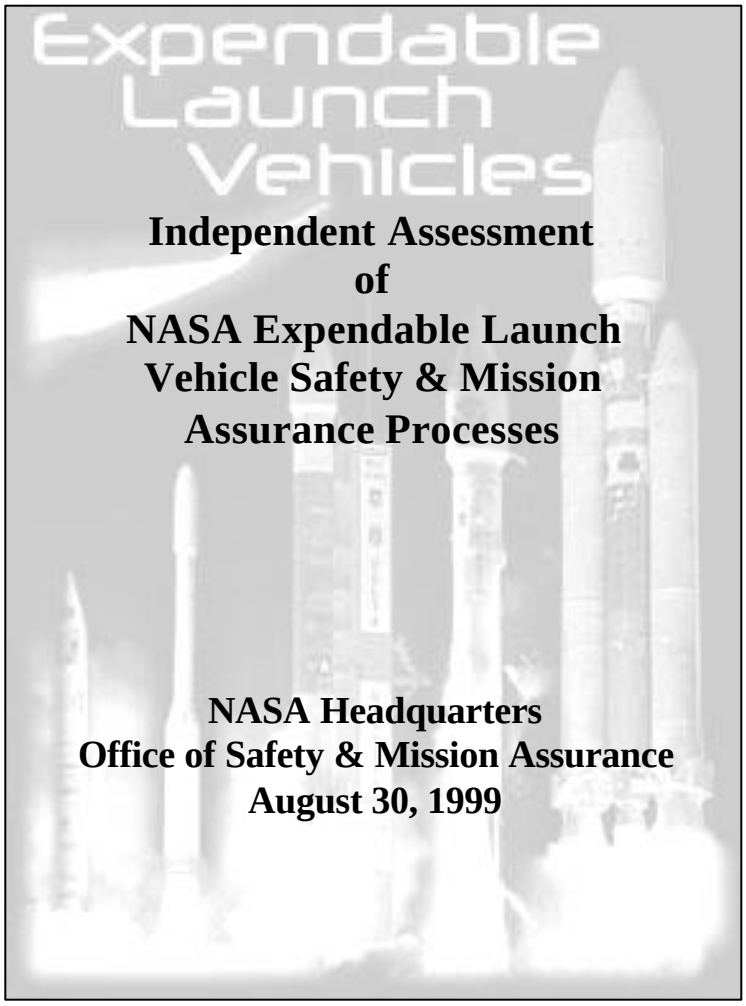
This document contains excerpts from the Expendable Launch Vehicles (ELV) Independent Assessment Report (title page shown below). Only those sections which relate to the PBMA element **Hardware Design** are displayed.

The complete report is available through the PBMA web site, Program Profile tab.



3.2 Probable Causes and Assurance Process Gap Analysis

ELV Failure Case Studies and Gap Analysis

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
2.	**Titan IV-A20: 12 Aug 98-Booster Cable Short** Intermittent shorts on vehicle power bus. Harness insulation was flawed prior to launch and escaped detection during preflight inspections.	Fundamental design issue or poor quality workmanship on just this vehicle.	NASA/ELV Design Verification and/or Mfg. Verification Activities would not likely have detected these failures. DCMC would be most likely to detect the potential failure mode. DCMC supports both NASA and DOD.	Low
5.	**Athena: 27 Apr 99-Booster Fairing Failure** Shroud failed to separate. Shock unplugged electrical connection. Electrical signal not received.	Greater than anticipated shock associated with initial fairing separation resulted in incomplete final separation. Apparently a design defect - design verification and test failure. Coupled loads analyses should have fully characterized the separation event.	If the vehicle was qualified under NPD 8610.7 then KSC Engineering would not likely have required special fairing/separation qualification testing which might have detected the problem.	Low/Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
8.	**Atlas-Centaur (AC-62): 09 Jun 84-Upper-Stage Failed To Boost (NASA)** Leak occurred in the LO2 tank. Incorrect clearance between inter-stage adapter and tank. High pressure in tanks at separation.	Failure difficult to mitigate through insight processes.	NASA GRC managed pre-commercial assurance approaches employed at this time. Very unlikely that diminished "insight role" would have detected.	Low
9.	**Titan 34D (D-7): 28 Aug 85-1st Stage Engine Shut Down (DoD)** Large oxidizer and fuel leaks and turbopump assembly failure.	Three separate and independent failures. Corrective actions were design changes and manufacturing processes.	NASA/ELV design verification and mfg. verifications not likely to have prevented this launch failure.	Low
10.	**Delta 178: 03 May 86-1st Stage Shut Down (NASA)** Electrical short in electrical relay box. Lack of redundancy, added relays, and second 28-volt power source.	Corrective actions were primarily design changes.	Failure occurred under GSFC (NASA oversight mode of operation). Current NASA/ELV design verification processes not likely to find flaws.	Low
15.	**Atlas-Centaur (AC-70): 18 Apr 91-One Centaur Engine Did Not Achieve Full Thrust** Air ingested into the turbo-pump liquefied and froze in the C-1 engine LH_2 pump and gearbox.	Failure difficult to detect by any secondary insight process. Design and new inspection/procedural corrective actions. New inspections and procedural changes were identified to eliminate debris in the fuel line.	NASA/ELV design engineering processes would have looked closely at a design change. Non-design change failure mode (latent defect) in design would not likely have been detected.	Low

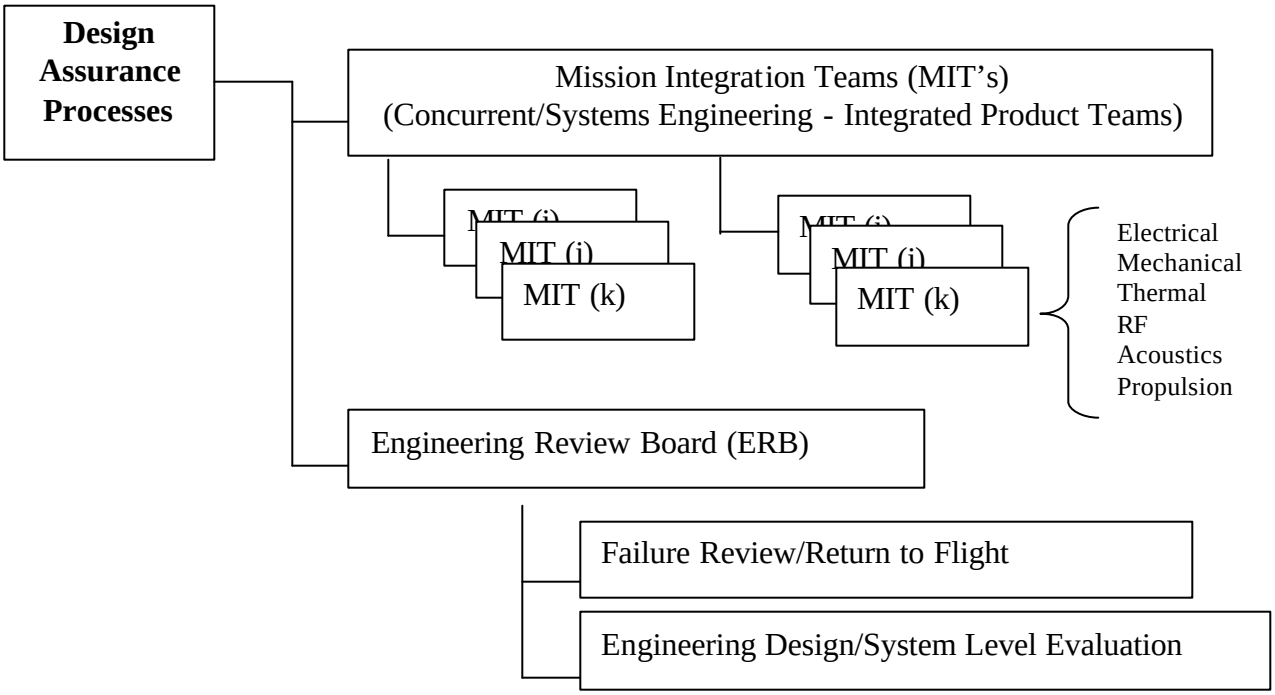
	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
16.	**Pegasus (F-2): 17 Jul 91-Incomplete 1st/2nd Stage Separation** Increased linear shaped charge, added spacer to protect charge detonation block. Fairing hinges strength increase and weather seal redesigned.	Design deficiencies. Low probability to detect failure.	NASA/ELV design engineering and design verification processes may (or may not) have identified failings in a new/modified design launch vehicle.	Low/Medium
17.	**Atlas-Centaur (AC-71): 22 Aug 92** Centaur C-1 engine failed due to the ingestion of air into the turbo-pump.	Difficult failure scenario to detect. Design and new inspection/procedural corrective actions.	NASA/ELV ERB would have carefully considered return to flight rationale, although a latent design defect would not likely have been detected by NASA/ELV engineering activities.	Low/Medium
18.	**Atlas-Centaur (AC-74): 25 Mar 93-1st Stage Thrust Loss** Regulator problem. Inefficient burning of fuel at lower throttle setting used up propellant.	Corrective actions were design changes (regulator redesigned) in a mature launch vehicle (latent defect).	NASA/ELV design engineering processes would have looked closely at a design change. Non-design change failure mode (latent defect) in design would not likely have been detected.	Low
20.	**Pegasus XL (STEP-1): 27 Jun 94-Inaccurate Estimation Of The Vehicle Aerodynamics**. Erroneous aerodynamic predictions were used to design the flight control autopilot system. Insufficient design verification testing.	Too great a dependence on analysis and modeling coupled with marginal validation of model are root causes.	For first-time vehicle use or newly qualified vehicles there is a greater likelihood that KSC ELV engineering would detect this design defect.	Medium

	ELV Failure Description	General Comments	NASA ELV Assurance Process Or Activity That May Have Prevented This Mishap	Subjective Assessment High/Medium/Low Probability of Mishap Prevention
22.	**Delta 228 (Koreasat-1): 05 Aug 95-One of nine SRM's Did Not Separate** Malfunction in the separation explosive transfer system. Overheated thin layer explosive transfer lines.	Separation system design changes (4 items) identified as corrective actions.	NASA/ELV design and engineering processes would not likely have identified these failure modes.	Low
23.	**LMLV-1 (DLV): 15 Aug 95-Thrust Vector Actuation Mechanism Malfunctioned** Erroneous feedback signal caused by reduction of electrical resistance in cables. Cables heated by hydraulic oil ignition. Redesigned hydraulic oil expulsion, improved thermal protection for cables and TVA components.	Three fundamental design failures contributed to vehicle loss. Improper design verification testing is a contributing factor.	NASA/ELV design and engineering processes would not likely have identified these failure modes in a commercial launch mode. If qualifying vehicle for first flight it is possible that NASA would have identified design problems.	Low/medium
24.	**Conestoga 1620: 23 Oct 95-Unintended Thrust Vector Actuation Signal Was Sent To The Castor IVB Nozzle Actuator** No software filters to reduce noise to the onboard navigation computer.	Fundamental design flaws in hydraulics, software, and vehicle modal analysis. Latent design defects. If first flight or qualification flight NASA MSFC (in support of KSC engineering) may have detected design defects.	NASA design/engineering may or may not have identified failure modes in initial vehicle qualification. Post initial qualification NASA would not have been in a mode to capture a latent design defect.	Medium

A.3 Design and Engineering Assurance Processes

Introduction

Design and engineering assurance processes are considered those systems engineering disciplines and methods that tend to mitigate or control design risks. The NASA ELV Program office employs a concurrent engineering approach centered on the activities of the Mission Integration Teams and the Engineering Review Board. Neither process is yet formally documented with a KDP but both processes are well understood by participants and serve to achieve the benefits of a system level engineering perspective.



Mission Integration Team (MIT) Approach

Mission integration is the primary responsibility of the Mission Integration and Customer Division and is accomplished through the formation of MIT's (see figure A-2) which are established for each individual mission. The MIT serves as the link between the spacecraft customer and the launch vehicle service provider. The Mission Integration Manager (MIM) leads the MIT and is supported by an Integration Engineer, who provides discipline engineering, mission analysis, and mission assurance; a Launch Service Manager, who provides procurement and finance support; and a Launch Site Integration Manager, who is responsible for range and launch operations support. The MIT assumes total management of the mission integration process. The MIT becomes involved in the integration process very early by providing mission analysis and feasibility study support in the pre-Announcement of Opportunity (AO) and AO phases of mission selection. One team is established per mission with core team membership

drawn from the ELV Program. The MIT, typically established 30 to 36 months prior to launch, serves as the principal customer point of contact and the launch services mission point of contact.

Once a mission receives Authority to Proceed (ATP), the MIT uses the following forums to refine mission requirements:

- Mission Integration Working Groups (MIWG's)
- Preliminary/Critical Design Reviews
- In-plant Product Reviews
- Design Certification Review

Integration and other issues are reported and tracked through:

- Weekly Project Status (ELV Program Internal)
- Monthly Status Report (ELV and Spacecraft Project Report)
- Quarterly Program Reviews
- Technical Interchange Meetings
- Readiness Reviews (NASA and contractor)
- Engineering Review Boards

The process allows both the Government and the launch service provider the opportunity to work the closure of any issue through the Launch Readiness Review (L-1). If an issue cannot be closed prior to the start of the launch countdown, the ELV Launch Services Project will not consent to proceeding with the launch.

MIT Lessons Learned - The Mission Integration and Customer Division also employs an internal review, lessons learned/continuous improvement process. This process involves formally logging actions, identifying individuals to address those actions, and tracking closure of the actions. Typical ELV lessons learned include:

- issues which may have fallen through the cracks requiring additional oversight by management
- areas which could benefit from better coordination of MIT team activities
- areas where confusion may have existed
- areas requiring extra emphasis in MIWG's preparation activities
- areas where improved communication is important
- issues associated with timing and schedule margin
- the need to develop a process or schedule
- the need to determine who is responsible and has authority to address closure of issues
- other "out-of-standard process" issues

The lessons learned forum also serves to identify strengths and positive outcomes from previous launch campaigns.

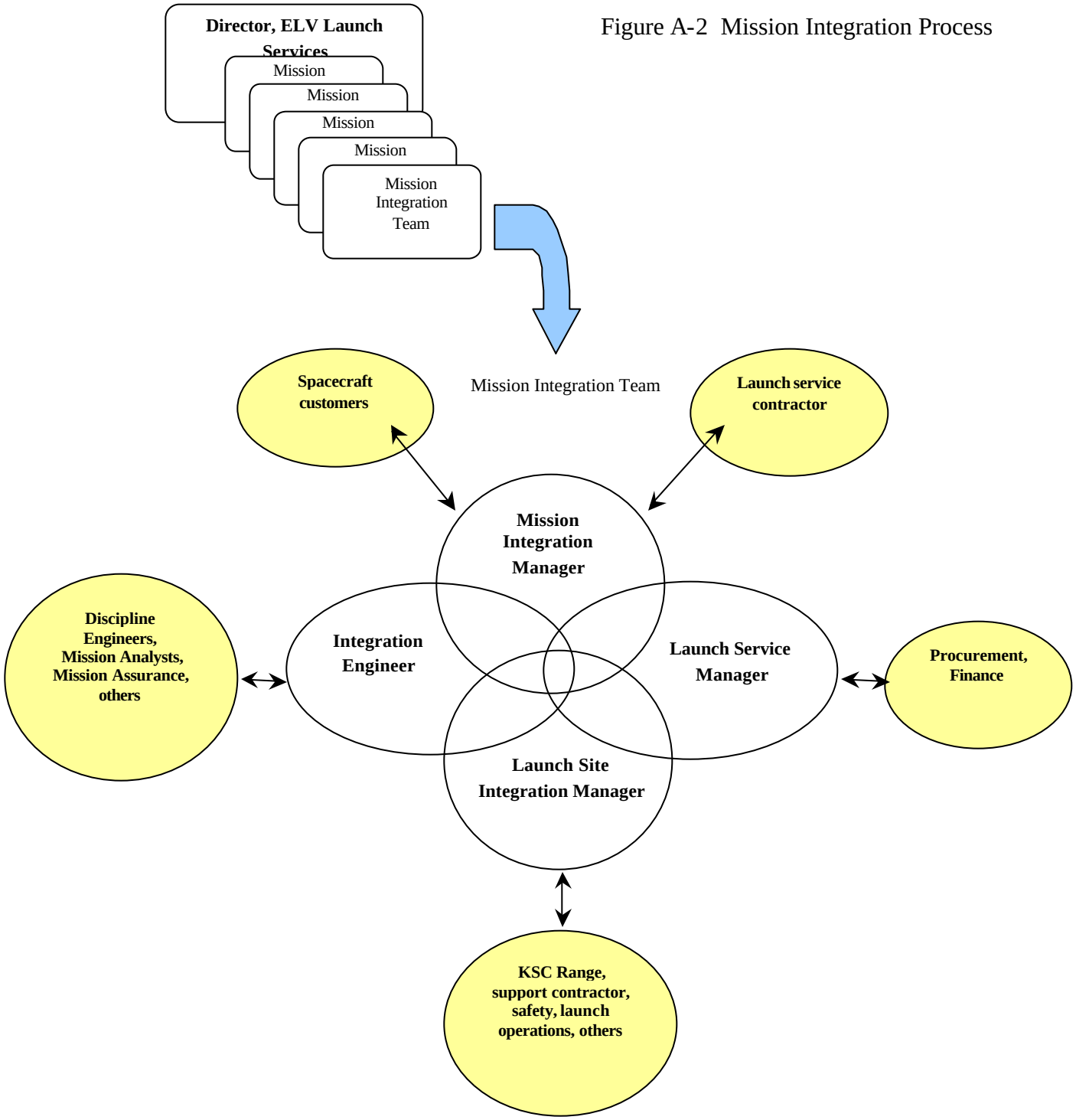


Figure A-2 Mission Integration Process

Engineering Review Board (ERB)

The ELV Launch Services Vehicle Engineering and Analysis Division employs an ERB as the principal technical engineering risk management forum. The independent ERB does not consider cost and schedule but seeks to identify the best technical course of action. An ERB is convened when a systems level evaluation is required for issues raised by any individual within the engineering or integration organizations. Throughout the mission integration process, engineers will identify and resolve problems through analysis, test, and technical interchange meetings. Typically two to three issues are identified each week as potential ERB candidates. The KSC/ELV ERB process derives from both the GRC and GSFC ELV Program management heritage. The ERB process, while routinely implemented, has not yet been formally documented (with a KDP) and is not incorporated under the KSC/ELV ISO 9001 certification.

Membership - The ERB is chaired by the Vehicle Engineering and Analysis Division Chief Engineer. The four other permanent ERB members are drawn from within the Vehicle Engineering and Analysis Division including:

- Chief, Vehicle Engineering and Analysis Division
- Chief, Mission Analysis Branch
- Chief, Mechanical Systems Branch, or Chief, Avionics & Electrical Branch
- Chief, Engineering Integration Branch, or Integration Engineer (Mission Specific)

Prior to April of 1999 there were no ELV/Flight Assurance Managers (FAM's) at KSC. It is the intent of the Chief Engineer to seek SMA/FAM participation in future ERB meetings. It is also important to note that contractors and other interested/contributing individuals and organizations may be invited to attend ERB discussions.

Criteria for Establishing an ERB – The informally implemented ERB start up criteria include:

- ELV launch service provider request for engineering evaluation
- Class-1 (form, fit, or function) changes to the core vehicle
- Changes in any aspect of core or mission-peculiar hardware or software
- In-flight anomaly and return-to-flight rationale development

Return to Flight Rationale – The ERB has a track record of exercising care and due diligence in evaluating and accepting contractor logic and rationale to support return-to-flight decisions after the occurrence of a mission failure. The fundamental engineering concept and NASA cultural norm of never flying with a known unknown serves as starting point for ERB deliberations. The ERB attempts to establish knowledge and understanding (to the greatest extent possible) of what went wrong, what failure mechanism(s) contributed to the mishap, and what design, manufacturing, or operational changes have been implemented to mitigate the likelihood of reoccurrence. In addition to ERB evaluations and recommendations, the KSC Center Director may empanel outside experts to independently review and evaluate recommendations developed by the KSC/ELV/ERB, the ELV launch service provider, and other consultants (e.g., Aerospace

Corporation) before approving a return-to-flight status.

Engineering Decisions – As shown in figure A-3, once the ERB has addressed a technical issue, it submits recommendations to the appropriate MIT/MIM. In the event of a technical disagreement between the ERB and a MIT or MIM the Project Decision Meeting (PDM) forum can review the issue, although this would be a rare occurrence. The PDM also serves as a forum to discuss technical issues with fleet-wide implications and serves as a necessary step in the process of acquiring funding to address issues which are out of scope for the MIT funding in excess of $200K. Actions requiring funding levels in excess of the $200,000 threshold require submission to the Program Requirements Change Board (PRCB) chaired by the Chief, Program Integration Office.

Engineering Review Board Interactions

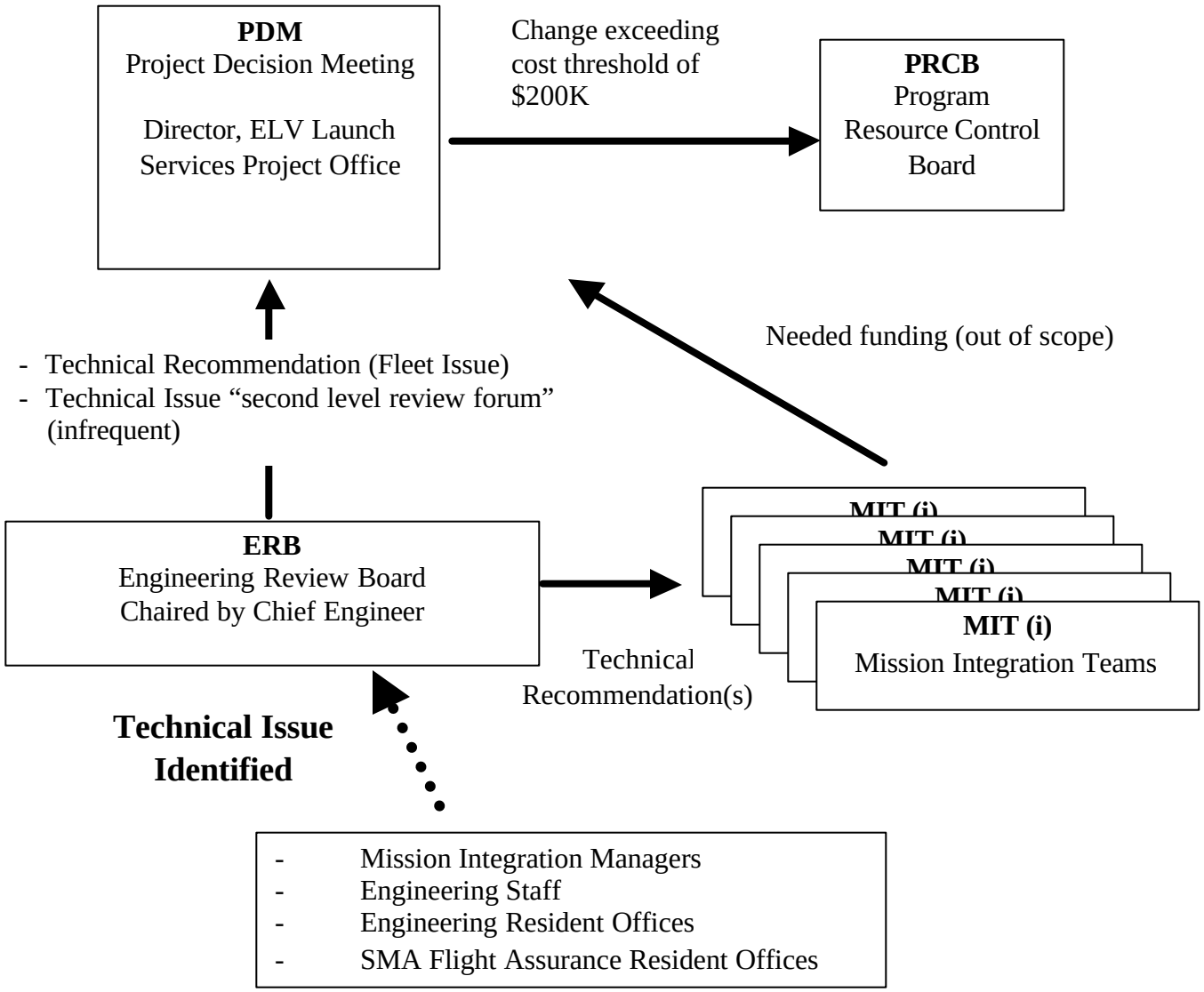


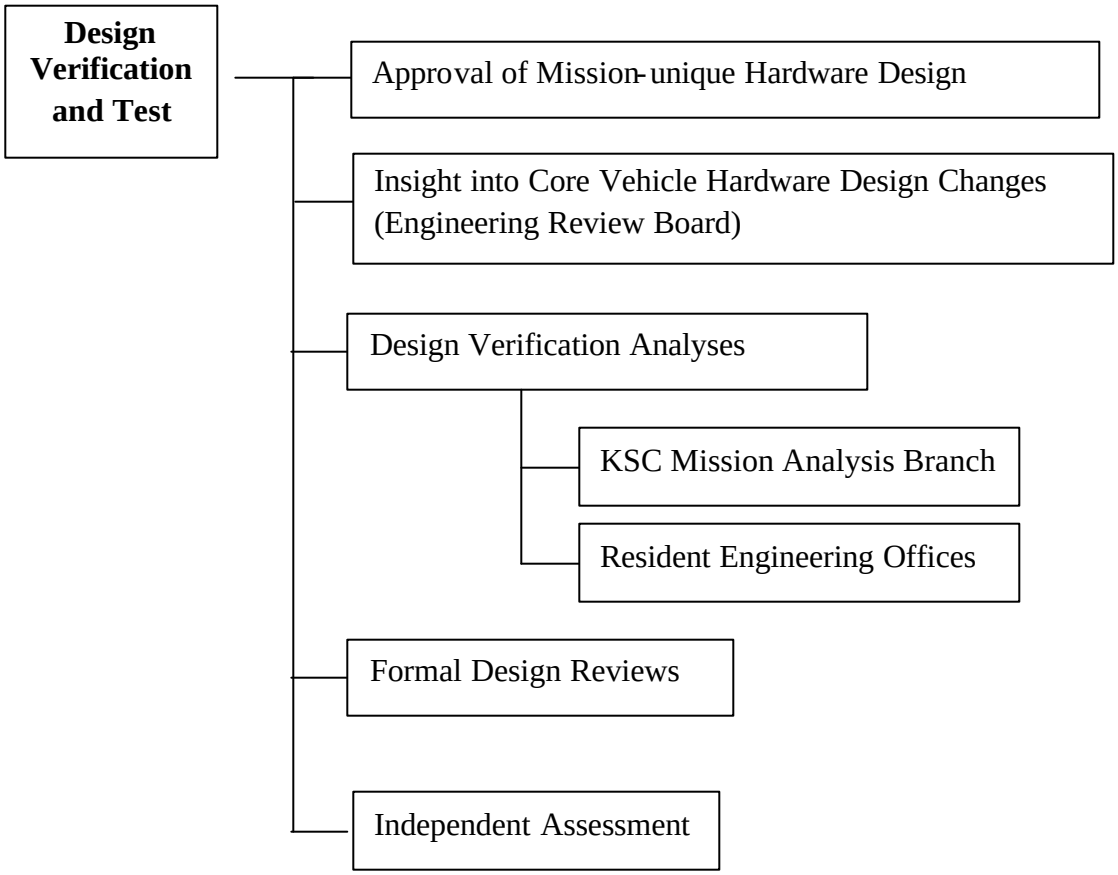
Figure A-3

A.4 Design Verification and Test Assurance Processes

Introduction

NASA ELV design verification processes represent a key strength in the NASA ELV management approach. Design verification processes include:

- approval of mission-unique hardware and software design
- insight into core vehicle hardware design changes
- verification of design through analysis
- use of design reviews (formal boards)
- use of independent design verification consultants and teams



Approval of Mission-unique Hardware Design

NASA KSC-based and in-plant engineering and flight assurance personnel directly participate in engineering decisions related to NASA mission-peculiar hardware and software. The resident offices serve as the first line of contact and interaction for production and design engineering insight. Residents participate in vehicle integrated product team activities, telecons, and meetings. KSC-based subject matter experts,

essentially matrixed into individual programs in-work, participate on an as-needed basis. These KSC-based engineers also participate with engineering residents in telecons and video-conferences to work specific issues. KSC/engineering residents also participate in Mission Integration Working Group (MIWG) activities.

LMA/Cassini (Titan IV) Example - Engineering and flight assurance participation begins at the earliest possible moment in the design phase of the (mission-unique) spacecraft/launch vehicle Interface Control Document (ICD). The following activities involved both lead-center engineering (GRC at the time), in-plant engineering, and flight assurance.

- Participation in the original integration contract requirements definition and the Memorandums of Agreement between the Air Force and NASA

- Participation in the draft, approval, and revision process for the Cassini Interface Control Document (ICD) and the Program Requirements Document (PRD). The ICD (an LMA Document) is used to identify all the interfaces between the launch vehicle, spacecraft, and the launch pad. The PRD (an LMA document) defines the requirements at the launch site for Cape Canaveral Air Force Station (CCAFS) facilities, including the launch pad itself.

- Participation in the development and design reviews related to incorporation of the ICD requirements, for both integration hardware and requirements, both stated and derived.

- Tracking and coordinate the initiation of Interface Verification Completion Reports (IVCRs) for the ICD.

Insight into Core Vehicle Hardware Design Changes

Baseline vehicle design and engineering is the primary function and responsibility of the vehicle manufacturer/launch service provider. It should be noted that, in practice, the level of NASA insight varies as a function of the particular ELV launch service provider. The NASA ELV Program Office and SMA organizations at KSC have minimal direct input to, or influence on, the basic design and engineering of the core vehicle. However, they do have "insight" responsibilities, as defined in the current NMI 8610.23, which include participation in meetings, tests, data reviews, reports, inspection records, analyses, and simulations. Ideally the "insight process" enables an understanding of the hardware, software, and management processes used by the launch service provider in the design, analysis, test, launch, and operation of the vehicle.

NASA core vehicle insight is accomplished through the activities of field resident office engineers, KSC cognizant discipline engineers and flight assurance managers. Insight is achieved through access to manufacturers meetings, records, and production facilities. Insight includes witnessing tests, attending reviews and meetings, reviewing documents, and conducting limited analysis. Insight does not involve an approval role. Most importantly, insight is limited by the resources available, primarily staffing. Insight activities identified in NMI 8610.23 include:

- baseline vehicle design, analysis, and configuration management
- design and qualification reviews
- production program reviews, plans, and schedules
- production and system test material review boards
- SMA compliance evaluations
- system tests, post-test data, anomaly resolutions, and failure analyses
- walkdowns, launch site schedules, and plans
- ground support equipment procedures
- work practices and documentation
- post-flight vehicle, tracking, and range data
- post-flight anomaly investigations and closeouts

Design Verification Analyses

Design verification represents an area in which policies and procedures to identify "how deep" and "how wide" are still in development. This is a natural occurrence, representing the merging of two somewhat different design verification philosophies. The GRC-heritage approach, where they typically managed one-of-a-kind, highly complex payloads (Titan and Atlas launch vehicle), was to conduct comprehensive design reviews. The GSFC heritage (Delta and Pegasus) approach was to conduct comprehensive design reviews for first flight configurations, then reduce the number of reviews on reflights of proven designs. The KSC/ELV Program is developing a selective analysis approach based on consideration of payload complexity, cost, uniqueness, and prior NASA analysis verification history for the launch system.

NASA KSC-based engineering and flight assurance personnel directly participate in test planning and review test data developed to verify the design of NASA mission-peculiar hardware. Contractor analyses are routinely reviewed by the NASA engineering team (residents and KSC-based). The NASA assurance approach, or philosophy, is to develop confidence in the contractor's design tools, techniques, and practices.

Depending on the specific contract clauses, independent analysis may form the basis of NASA approval of the contractor design. In selected cases, NASA engineering will conduct independent analysis to validate contractor design activity. ELV engineering and flight assurance personnel, as a matter of practice, conduct no independent analysis of core vehicle engineering. They do, indeed, conduct independent analysis in the case of unique or technically challenging modifications to the vehicle necessary to support NASA requirements. Independent analysis may also be conducted for selected first flight items or subsystems that may have been involved in an in-flight anomaly.

The launch service provider has primary responsible for conducting typical design verification (system/component testing, flight environmental testing, integrated tests, analyses, similarity testing, simulations, etc.) and reviews.

KSC Mission Analysis Branch - The KSC-based Mission Analysis Branch provides ELV analytical support in the following areas:

- Trajectory and Performance
- Guidance Accuracy, and Flight Software
- Guidance, Navigation, and Control Dynamics
- Coupled Loads
- Structural/Stress Analysis
- Environments: Acoustics, Thermal, Shock, and Vibration

Independent analysis is conducted for selected mission-unique items. The decision is typically based on the complexity of the mission.

Currently, an attempt is made to address each of the above areas for every mission, however, due to staffing limitations the question becomes one of depth and level of detail. The expressed concern involves the expectation of providing, with a minimal staff, the same level of insight and independent analyses for every mission including repeat missions and missions which are similar in nature. As noted before, this issue is related to both increasing staff and providing appropriate skill mix.

The Mission Analysis Branch has been able to staff with experienced analysts in critical areas including trajectory/flight design, coupled loads, guidance and controls, stress analysis, and flight software. The available expertise in these areas is primarily a result of consolidation within NASA with several analysts having transferred to KSC from GRC and GSFC. ELV heritage experience includes performing IV&V activities for GOES, SOHO, EOS, Cassini. The analysis branch workforce presently includes:

- Trajectory and Performance: four experienced analysts plus two in training
- Guidance Accuracy and Flight Software: two experienced analysts plus one in training
- Guidance, Navigation, and Control Dynamics: two experienced analysts plus one in training
- Coupled Loads and Vibration Environments: four experienced analysts
- Structural/Stress Analysis: one experienced analyst
- Acoustic Environments: one experienced analyst
- Thermal Environments: one analyst in training

The branch is working to get all relevant codes and models in place at KSC so that they may be used when needed. Guidelines for when IV&V is performed are still being developed. It is anticipated that the criteria will reflect mission complexity, cost, and maturity of launch vehicle.

Resident Engineering Office (Boeing/Delta Example) - NASA contractor engineering support staff covering Boeing/Delta assembly activities at the Pueblo facility routinely perform in-depth mechanical and electrical analysis on selected flight critical hardware to determine parametric sensitivities, margins, and stability. Hardware selected for analysis is typically based on out-of-family deviations, in flight critical component acceptance test data or system data, or manufacturer's uncertainty in environmental or control margins. Activities include structural and electrical analysis.

Formal Design Reviews

LMA/Atlas and Titan Example: NASA Engineering In-Plant Participation in Design Reviews Panels and Boards - The LMA design process used on Atlas and Titan launch vehicles typically employs the following design review forums.

- Systems Requirements Reviews
- Preliminary Design Reviews
- Critical Design Reviews
- Vehicle Engineering Review Boards
- Vehicle Software Reviews
- Vehicle Test Readiness Reviews
- Vehicle Build Reviews
- Vehicle Space Program Reliability Boards
- Vehicle Senior Engineering Review Panels

The NASA engineering resident office employs a matrix marker board approach to assure that each critical review is covered by one of eight engineering staff members. It is noted that KSC-based engineers also participate (remotely) in many of these Denver-based meetings as well.

Independent Assessment

Independent assessments are part of NASA's willingness to ensure all management, technical, administrative, manufacturing, operational, and failure investigations issues have been resolved and independently reviewed. For example, independent teams were chartered for the upcoming Terra launch, NASA's flagship earth observation system mission and the Cassini launch, NASA's space science mission to Saturn.

LMA/Atlas Terra - A 12-person team, representing 400 years of experience, examined the KSC and GRC launch service management process during KSC's transition as NASA's lead center for ELV launch services. This team examined current ELV insight approval processes, launch site operations, first flight items, unique Terra interfaces, and ELV program transition shortcomings. The team found that the Terra insight/approval process supported the flight worthiness of the Terra AC-141 launch and the KSC/GRC process was consistent with expectations for flight worthiness.

LMA/Titan IV: Cassini Mission - The Cassini space science mission was another NASA program which receive special review atypical of most commercial or government

launches. Powering the Cassini spacecraft to Saturn, the spacecraft has three radioisotope thermoelectric generators or RTGs, which contain plutonium-238 to generate direct current electricity. The Cassini launch must passed interagency nuclear safety review requirements. Teams from both Jet Propulsion Laboratory and KSC scrutinized the launch vehicle. In addition, an External Independent Readiness Review (EIRR) team was established for Cassini. Under NASA EIRR contract, Aerospace Corporation of El Segundo, CA, reviewed the design and build of the major Titan IV vehicle components flown for the Cassini mission. Special attention was given to the solid rocket motors. This included oversight of all activities at the solid rocket motors contractor facility including build and propellant casting of segments.